[19]中华人民共和国专利局

[51]Int.Cl[6]
G06K 9/00

[12] 发明专利申请公开说明书

[21] 申请号 97100712.8

[43]公开日 1997 年 10 月 1 日

[11] 公开号 CN 1160891A

[22]申请日 97.2.5

[30]优先权

[32]96.2.5 [33]US[31]08 / 596570

[71]申请人 苏格波尔公司

地址 美国加州

[72]发明人 周维贤 汤瑞龙

[74]专利代理机构 中原信达知识产权代理有限责任公司

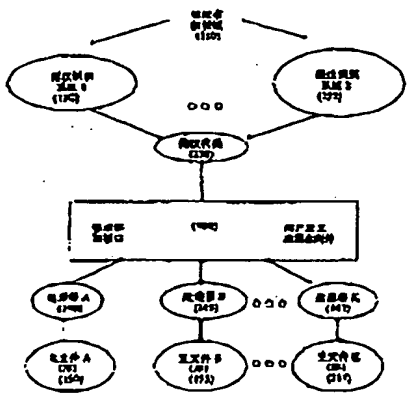
代理人 余 朦

权利要求书 3 页 说明书 8 页 附图页数 3 页

[54]发明名称 在保密业务中使用指纹数据的个人识别系统

[57]摘要

本发明提供了一种在保密敏感业务中使用指纹数据的个人识别系统，按下列步骤进行：产生一个用于规定多个不同比率("CR") 等级的存取文件，其对应于一种可接受的业务；接收请求者的指纹数据和其伴随的请求参数；将该指纹数据与请求业务的帐户对应的主文件中多个指纹数据之一比较；根据比较结果产生 AR / RR；使用该存取文件评估业务请求和 AR / RR；如果 AR / RR 适合于所请求的业务，在成功地通过附加鉴别测定之后批准该请求，如果 AR / RR 不适合于该业务，至少进入一个附加鉴别的例外程序。



权 利 要 求 书

1. 在基于指纹进行保密数据业务的系统中，包括：

至少一个指纹识别装置，用于以预定格式识别和产生请求者的指纹数据，

主文件和库，用于最初存储与所述系统的多个用户对应的多个指纹数据，和

一个耦合到所述主文件和库的数据处理单元，通过采用所述预定标准将来自所述请求者的所述指纹数据与所述主文件和库中的对应项目比较，为所述请求保持所述主文件和库中保存的预先建立的标准，一种所述系统的个人识别方法，利用所述请求者的所述指纹数据进行保密数据业务，包括步骤：

a)为每个帐户产生并保持一个用于规定多个不同 AR/RR 等级的存取文件，每个等级对应于一个可接受的业务，以便当满足 AR 等级时允许进行业务，或当其低于 RR 等级时拒绝该业务；

b)接收请求者的指纹数据和其伴随的业务和帐户信息请求；

c)为所述请求者的指纹数据产生一个 CR；

d)将所述请求者的所述指纹数据和与所述帐户有关的所述主文件中的所述多个指纹数据之一比较；

e)使用所述存取文件对照所述 AR/RR 评估业务请求的所述 CR；

f)如果所述 AR 适合于所述请求，批准所述请求；如果所述 CR 不适合于所述业务，至少进入一个用于附加鉴别的例外程序。

2. 根据权利要求 1 所述的方法，所述步骤 f)进一步包括至少进入一个由帐户用户预先定义的用于附加鉴别测定的例外程序的步骤。

3. 根据权利要求 1 所述的方法，所述进入至少一个例外程序的步骤 f)包括至少下列步骤之一：

a)评估一组预定的例外规则以补充鉴别；

b)从所述请求者请求附加信息以补充鉴别；

c)请求第三方介入以补充鉴别。

4.根据权利要求 2 所述的方法，所述进入至少一个例外程序的步骤 f)包括至少下列步骤之一：

a)评估一组预定的例外规则以补充鉴别；

b)从所述请求者请求附加信息以补充鉴别;

c)请求第三方介入以补充鉴别.

5. 一种便于执行保密数据业务的个人识别系统, 包括:

输入装置, 用于从请求者接收业务请求, 所述业务请求伴随着从用于识别所述请求者指纹的指纹识别系统产生的所述请求者的指纹, 以便以预定格式产生所述请求者的指纹数据;

库和主文件, 用于存储与多个帐户拥有者有关的多个指纹数据, 所述主文件和库还登记多个业务所需的多个保密等级作为针对每个帐户拥有者的初始规定;

耦合到所述库和主文件以及所述输入装置的数据处理装置, 用于将所述请求者的指纹数据和与所述帐户对应的所述主文件中的项目比较, 所述数据处理装置根据预定比较标准产生一个比率("CR");

耦合到所述主文件的请求评估装置, 用于确定所述 CR 是否满足所述业务请求所需的预定保密标准, 如果肯定, 则在成功地通过至少一个预定例外测定之后批准所述请求;

耦合到所述请求评估装置的例外处理装置, 如果所述 CR 不满足附加鉴别的所述预定保密标准, 用于产生预定接受规则, 如果所述 CR 不满足附加鉴别的所述预定保密等级, 所述例外处理装置也产生一组预定的拒绝规则用于产生预定接受规则.

6. 根据权利要求 5 所述的系统, 其中所述例外处理装置进一步至少包括下列之一:

提醒间接方介入的装置;

提醒直接方介入的装置;

用于请求所述用户提出附加信息以补充鉴别的装置;

使所述机构建立定制的自动例外规则和步骤以补充鉴别的装置.

7. 根据权利要求 6 所述的系统, 进一步包括:

耦合到所述输入装置和数据处理装置的用户定义装置, 用于在不批准请求时定义多个预定处理功能.

8. 可由机器读取的程序存储装置, 可通过机器执行而确实实施的指令程序, 以执行用于实施在前端和后端之间进行保密业务的个人识别系统的方法的步骤,

前端包括用于读取用户指纹以便以预定格式产生指纹数据的指纹

识别单元，和用于接收用户的指纹数据和针对保存在后端的帐户的业务请求的输入单元，通过用户的指纹数据初始建立该帐户，

后端包括用于保存所述帐户并将来自前端的指纹数据与由业务请求识别的所述帐户的指纹数据进行比较的数据存储和处理单元，后端通过将前端接收的指纹数据和与该帐户相关的指纹数据比较产生一个比率("CR")，该方法包括步骤：

a)为该帐户建立多级存取文件，该存取文件表示多个可允许业务所需的多个保密标准；

b)向多级存取文件提供至少一个例外处理的至少一个等级，当所述 CR 低于可允许业务的要求时启动例外处理，例外处理启动时，该例外处理产生多个由用户定义的功能和作用；

c)在后端存储该多级存取文件和例外处理，以便在后端接收业务请求和来自前端的用户指纹数据时可启动存取文件和例外处理。

9. 根据权利要求 8 的计算机程序，其中例外处理至少包括下列步骤之一：

a)向用户请求附加信息以补充鉴别；

b)通知本地第三方介人；

c)通知远端第三方介人。

10. 根据权利要求 5 的计算机程序，其中如果 CR 满足所述预定保密，所述例外处理装置也产生附加预定接受规则，其中所述附加预定接受规则要求帐户拥有者提供附加核实。

说　明　书

在保密业务中使用指纹数据的个人识别系统

本发明涉及个人识别系统，特别是涉及通过指纹图象识别来鉴别用户的那些系统，以便于保密业务。

随着以用于金融业务的自动提款机(ATM)为例的自动交互机的激增，已对用于鉴别用户的更可靠的个人识别系统出现需求，这些用户希望在无人干预的情况下远程和自动地进行业务。按常规，人们简单地将其 ATM 卡插入机器使机器读取其帐户信息和密码，或 PIN("个人识别号码"，在此可与名词"密码"交换使用)。然而，随着整个日常生活变得更加自动化并具有保密意识，人们必须经常管理各种不同的密码和 PIN 以存取其银行帐户、其家庭安全系统、或其电子邮件帐户，在此仅列举几个为例。现有个人识别系统的复杂性已成为信息过量的原因之一，以致于没有 ATM 的正确密码可能会拒绝合法用户存取其帐户或其在线经纪人帐户。

人们经常忽略加在提供通过顾客密码或 PIN 存取的在线、或远程业务的金融机构的负担。当顾客忘记其 PIN 或顾客请求更改其 PIN 时，保存密码或 PIN 会迫使金融机关分配附加设备和人力资源以管理与顾客的联系。

另外，已经证实密码已不足以防止欺诈行为，可能的罪犯所需全部内容仅是一张 ATM 卡和其密码，而这两项内容很容易在那些不谨慎的人的范围中得到。除如上所述的复杂性之外，这是说明现有个人识别有何缺点的第一个实例。

另一个问题困扰着想象中应是安全的金融业务的完善性，有时有的帐户拥有者通过首先存取其帐户，过后即使在交易发生后仍否认该业务来欺骗金融机构。关于这类可恶行为的范围是有限的，即使考虑到仅占 ATM 业务较小的百分比也相当于一个较大的总和。没有更可靠的识别系统，金融机构必须消减该损失或将损失转嫁到其余顾客身上，从而提高每个人从事商业的成本。

除 ATM 业务之外，随着个人计算机和电信硬件和软件可供给能力的提高以及采用先进技术，人们很可能不久就会使用 PC 、调制解调器和诸如奇迹(prodigy)和互连网络等之类的公共电话交换网存取许多信息或进行各种保密业务，从而使鉴别成为该行业要处理的最头等重要的任务。

一种简单的个人识别系统涉及了上述问题。在许多年前就已知道指纹具有高度的准确性和可靠性，人们不会忘记指纹或将指纹与其它信息混淆。另外，一般来讲，罪犯不能偷走或复制人的指纹以模仿帐户拥有者。因此，指纹实质上是一一对应的个人识别，给定的指纹识别系统与信息革命一起发展。诸如 Identix 和 Startech 之类公司已开发了前端指纹图象识别系统以便可靠和准确地分析和识别指纹。

在后端，诸如 IBM 和 AT&T 之类主要的处理器供应商已能提供与指纹图象识别连接的系统，这样，金融机构可连接和访问大量指纹数据库，以快速鉴别其机器前的人，或借助调制解调器通过 PC 寻找以存取经纪人帐户的人。对于特定范围，当前的前端和后端供应商已经达到这样一种程度，而由某些行业，特别是金融行业完全利用其能力和成就仅仅只是时间问题。

即使在前端带有可靠的指纹图象识别系统，在后端带有快速响应处理器，该示例仍然存在问题。假设可合理地使 PC 所有者具有一个个人指纹识别装置以便提供在经纪人公司借助处理器对其在线经纪人帐户的存取以便于鉴别，由于人的指纹固有的不完善性造成仍然存在大约 1 %通常以合法用户被错误拒绝为特征的差错率。例如，如果一个人的日常工作是研磨化学制品，经历多年后其指纹质量趋于退化。当质量退化的指纹在最保密敏感业务中朝向保密敏感系统时，肯定会增加用户的苦恼，从而进一步侵蚀公众对未来系统完善性的信心。

另一方面，如果迫使保密敏感采用折衷方案以使错误"拒绝"最少，则可能增加错误"接受"的差错率，反之亦然。相反，如果迫使保密敏感采用折衷方案以使错误"接受"最少，则可能增加错误"拒绝"的差错率。既然折衷方案合宜的"匹配"允许存取错误。这即不是公众对基于指纹的个人识别系统的信心产生影响的措施。也不会有助于主要应用基于指纹的个人识别系统的行业保护其商业和金融利益。

此外，当帐户拥有者在金融机构的设备中借助其指纹首先设定其帐户时，可能不会完全分析形成的初始文件并作为文件数据存储。文件上具有不完整指纹的可能性很可能造成出现错误拒绝/接受。例如，如果初始登记为 90 % 的准确性，准确性则总是 90 %。即使以后的时间在 ATM 的读取 100 % 准确，最好的匹配仍为 90 %。换句话说，整个系统两端成为系统不可靠的原因之一。

因此，需要具有一种供指纹识别前端使用的个人识别系统，以提高准确性的百分比，从而使与保密业务有关的保密风险最小。

还需要具有一种采纳现有指纹识别装置优点的个人识别系统，以便根据前端和后端系统的各种自动出纳机提供灵活的解决方案。

还需要具有一种基于指纹的个人识别系统，提供易于用来解决存取信息超高速公路中所涉及的保密问题的方案。

本发明提供了一种在保密敏感业务中使用指纹数据的个人识别系统。该系统按下列步骤进行:产生一个用于规定多个不同比率("CR")等级的存取文件，每个等级对应于一个可接受的业务；接收请求者的指纹数据和其伴随的请求参数；将该请求者的指纹数据与请求业务的帐户对应的主文件中多个指纹数据之一比较；根据比较结果产生 AR/RR ；使用该存取文件评估业务请求和 AR/RR ；如果 AR/RR 适合于所请求的业务，在成功地通过附加鉴别测定之后批准该请求，如果 AR/RR 不适合于该业务，至少进入一个附加鉴别的例外程序。

下面的描述将使本发明的附加目的、特性和优点对本领域技术人员来说变得显而易见，其中:

图 1 是本发明高度简化的方框图。

图 2 是本发明的处理流程图。

图 3 是根据本发明的"建立屏幕"的一个实施例。

本发明提供一种采用指纹识别装置的个人识别系统。在下列描述中，以处理流程和功能方框图的形式公开本发明，其术语便于本领域技术人员理解。该术语也是使本领域技术人员在他们当中交流的手段。它即不限于特定的编码语言，也不限于特定的实施方法、硬件设备、操作

系统和操作环境．另外，本领域的技术人员应该理解，金融业务仅是可使用本发明的保密敏感业务的一个示例．正如将要理解的，本发明可应用于以鉴别进行存取的用户为结果的任何环境或业务．

参考图 1，该图示出本发明(100)按其所涉及的其操作环境高度简化的方框图．在前端，当诸如安装在 ATM 上的常用指纹识别装置之类的输入装置(200)接收请求者的指纹(110)时，这些指纹识别装置可分析、识别这些指纹并以预定的前端数据格式产生指纹数据(130)．来自不同自动出纳机的指纹识别装置(125)可产生不同的指纹数据格式(130)．这种情况表明存在许多指纹识别系统的前端自动出纳机，每个指纹识别系统根据其预定格式产生不同的指纹数据的情况．由于未建立和协调行业标准，接受不同指纹数据的每个处理系统必须将不一致的指纹数据转换成可用于和适用于由后端处理器系统存储和处理的指纹数据．在本发明(100)中，设置接口驱动器，每个驱动器针对于由各种指纹识别系统产生的各不相同的输入格式．另外，提供用户定义功能以使金融机构定制其独立的鉴别处理．

然而，应该指出，已建立了分析和识别指纹的方法．就此而论，本发明不依赖于下面将进一步描述的任何特定指纹识别系统．

在后端，有一个与存储指纹数据的主文件(150)的库有关的处理单元(140)．常规情况下是将来自前端的指纹数据(130)与主文件和库(150)中存储的指纹数据比较，以便根据某些预定的比较标准鉴别请求人．应指出，通常主文件指关于金融机构的帐户的所存储信息，而“库”是指由金融机构访问和保持的可执行程序和步骤．例如，金融机构可将输入装置从自动出纳机(120)链接到处理器(140)．因此，通常的初始任务将是通过已建立的协议确保两端可高效率和有效地进行通信．另外，将来可替代来自不同自动出纳机的指纹识别系统(125)，只要所产生的指纹数据可与主文件和库(150)中存储的指纹数据兼容或可转换成其中存储的指纹数据．

假设在前端和后端之间正确地建立了通信，本发明将在两端之间提供一个中间链路(100)，中间链路将不同的前端装置和数据统一成一种可接受和可识别的数据格式，本发明借助其内置的 AR/RR 逻辑等级和例外处理能力使整个个人识别方法更加简单和有效，并将其固有的 1 % 差错率降低到金融机构可接受的最低水平．

参考图 2，示出本发明的处理流程。当通过一组指纹(图 1 中的 130)接收存取请求时，分析和识别该指纹并随后用于产生指纹数据(200)。然后将所接收的指纹数据与目标主文件数据比较(205)以产生(210)一个比率(CR)。应指出，正如将由本领域技术理解的，根据指纹数据与主文件中的目标指纹数据比较如何可获得 CR，主文件上的目标指纹数据对应于预定标准下所提供的信息，例如帐号。还应指出，本领域的技术人员可便于定义如何表征比较结果，例如 50 % 匹配或 95 % 匹配。

目标主文件数据(205)可由一个专用 AR/RR 比率表、指纹数据和例外情况的表组成。专用比率表可允许本发明的金融机构或用户根据帐户拥有者的指纹可读性具有一个接受比率 AR 或一个拒绝比率("RR")。例如，帐户用户的指纹质量较差以致于仅能对该用户要求较低的专用 CR。

在拒绝或接受步骤两种情况中不论出现那一种情况，可实施或保持多个等级以便针对测定错误拒绝和错误接受的任何一种情况提供附加鉴别。

一旦确定 CR，例如 80 % 或 95 %，根据临界状态和显著阈值对照多级标准评估其伴随的存取请求(220)。如果 CR 满足该最低要求则继续评估。为降低错误接受的风险，金融机构还提供任选项以实施和保持内部附加测定(例如比较专门为帐户建立的附加组的标准)，或通过屏幕或用户接口从外部请求附加信息。附加信息可以是核实用户母亲婚前姓氏或核实附加密码。当通过标准阈值的最低等级时可认为评估成功。例如，如果请求者的 CR 为 70 % 并请求提取$30,000，则批准或拒绝该请求，假设帐户拥有者最初已允许该 AR/RR 等级的该业务。金融机构甚至可对任何超过$2,000 的数值设置更高的 CR 要求，这样对仅有 70%的 CR 的用户请求提取$30,000 会遭到拒绝。另外，应指出，当采用本发明建立其鉴别系统时，金融机构可借助多等级标准概念提供多个任选项和例外。

不同种类的业务需要不同等级的评估标准阈值。例如，对于检查帐户平衡的请求不需要 90 % 的 CR，并当帐户拥有者确定其帐户业务量时可由帐户拥有者设定较低的 CR 阈值，如果金融机构提供该特性的话。如同本领域技术人员可理解的，这种高度的灵活性减少了错误拒绝的机会，并使请求者的敌视性保持最低。应指出，可将不同标准保持并存储

在如上所述的表中(205).

为对本发明的个人识别系统进一步提供补充，为金融机构提供自动例外处理以介入所请求的存取．标准规则是针对多个等级(230 、 235 、 240)建立的(金融机构规定的)一揽子条件．正如众所周知的软件共用，例外是标准规则中未规定的特殊规则组．例外规则可以是辨别或对照例如金融、社会、地区、种族等地位等级的一揽子例外．或者可以是辨别或对照一个事件(例如特定日期/时间和场合)、或特有情况、事务或个人情况(例如具有特定金融状况或犯罪记录的个人)的专用例外．当不能通过 AR 测定的特定等级时，最低 CR(230)等级的例外处理(250)可自动核实与请求等级有关的所有例外标准，或当成功地通过 AR 等级测定时可自动核实对照请求．

当 CR 低于所要求的 AR，或当 CR 高于请求者的 RR 时，为进一步鉴别请求者可用另一个例外(255)要求补充存取码．例如，当由于输入装置不完善造成 CR 低于标准 AR 要求时，请求者可请求输入诸母亲婚前姓氏之类的附加信息以便仍能获得存取 ATM，而不是拒绝该请求．

可将通过 AR 的 CR 设定为"通过"测定，或可将其设定为执行专用于该请求者的附加例外测定．可针对预先设立的 RR 测定未通过 AR 测定的 CR．

如果 CR 下降到 RR 以下，可拒绝请求者，或可设定其执行专用于该请求者的附加例外测定．

如果 CR 未达到 AR 但超过 RR，可针对一揽子例外进一步评估 CR 以确定其资格．

在所有自动例外处理步骤已经用完之后作为极力要满足请求以及降低 AR/RR 差错率的手段，可由例外处理程序(260)将请求者附近的服务场所，例如分行，以使经授权的代表人工和直观地鉴别该请求．

如同本领域技术人员可理解的，通过 AR/RR 规则的任意组合以及多个例外处理(250 、 255 、 260)存在多个存取等级(230 、 235 、 240)，以使因固有的指纹数据不完善造成的错误鉴别最小．另外，本发明允许例如银行或经纪事务所之类的业务提供者机构确定如何建立和定制其

规则以及接受和拒绝的处理步骤．这些标准和例外的规则和步骤可在实施本发明的建立阶段期间由金融机构规定．该规则和步骤可由金融机构通过正式授权来保持．

图 3 说明根据本发明由金融机构遇到的"建立屏幕"．当建立帐户业务量时，在方框 300 定义各种工作功能．另外，在方框 305 定义附加功能．例如，前端硬件装置；基干硬件装置；网络环境；辅助功能；检查控制功能；加密功能；灾害恢复功能；报告写入功能；和实用功能．

在方框 310，金融机构可定义其标准 AR/RR 处理和标准．还可在方框 315、340 设立附加处理的任选项．例如，方框 315 可用于定义附加接受处理，方框 340 可用于义定义拒绝处理．这些附加任选项可设定多个 AR/RR 等级和其相应的例外处理(320、345、325、350、330、355)，即使带有标准 AR/RR310，金融机构可规定专用处理(306)，这些处理可包括信用检查、意外或紧急处理和专用的优先权许可．

根据本发明的个人识别系统可由软件方法实施．可通过 PC、EEPROM、和/或 CMOS，或其任何组合连接和控制其硬件和固化件．该系统和其方法为多等级和多维设计，从而保留了通用、灵活和可靠性．借助软件补充硬件控制可使常规差错率最小．

当本发明的装置内置于各种装置驱动器以连接各种不同装置，和内置于各种系统接口驱动器以连接各种操作系统时，该装置就其性质来说是独立的．规则和步骤的定制是具有手写能力的驱动菜单．例如，不同的金融机构可具有不同处理例外条件的方式．或者它们可根据其自身的人力和机器资源要求定制多等级结构．所有这些可通过使用菜单和书写功能完成．

其它实施设想如下：

1.装置独立
2.多级下拉菜单
3.例外处理出口
4.网络控制
5.内置检查控制
6.内置内部保密违章控制
7.数据加密/解密

8.灾害恢复测量和步骤(任选)

9.报告写人能力

10.指纹再匹配和文件保持等实用程序

虽然上面详细描述了本发明的几个示范实施例，本领域技术人员很容易理解，在不脱离本发明的新技术和优点实质的情况下可对该示范实施例做出许多改进。因此，其意图是将所有这些改进包括在如下面权利要求定义的本发明范围内。在权利要求书中，装置加功能的条款意图覆盖在此描述的作为执行所述功能的结构，结构等效不仅在于钉子采用圆柱形表面，在紧固木制部分的场合，钉子和螺钉可以是等效结构。

说 明 书 附 图

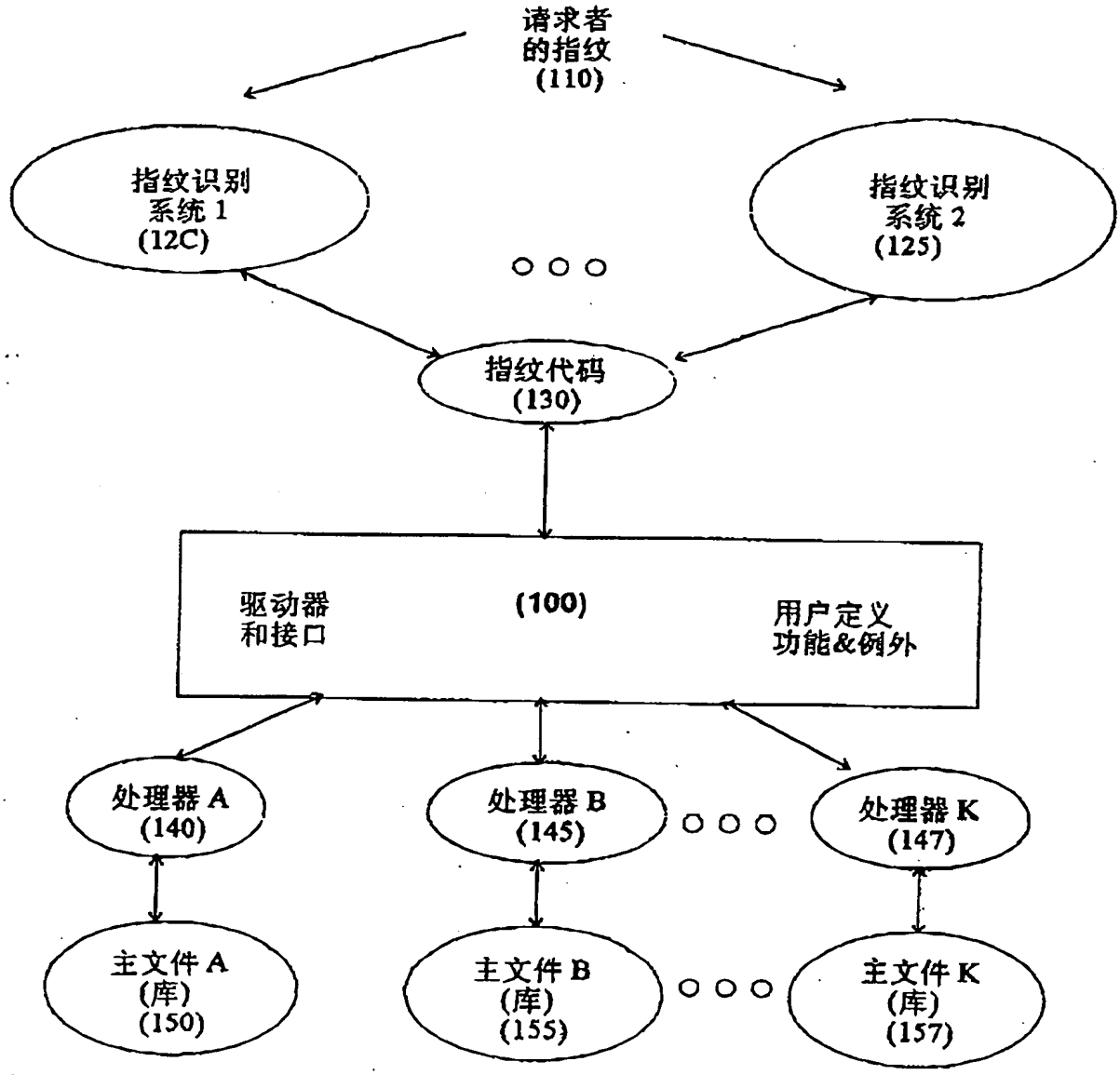

请求者
的指纹
(110)
指纹识别
系统 1
(12C)
指纹识别
系统 2
(125)
指纹代码
(130)
驱动器
和接口
(100)
用户定义
功能&例外
处理器 A
(140)
处理器 B
(145)
处理器 K
(147)
主文件 A
(库)
(150)
主文件 B
(库)
(155)
主文件 K
(库)
(157)

图 1

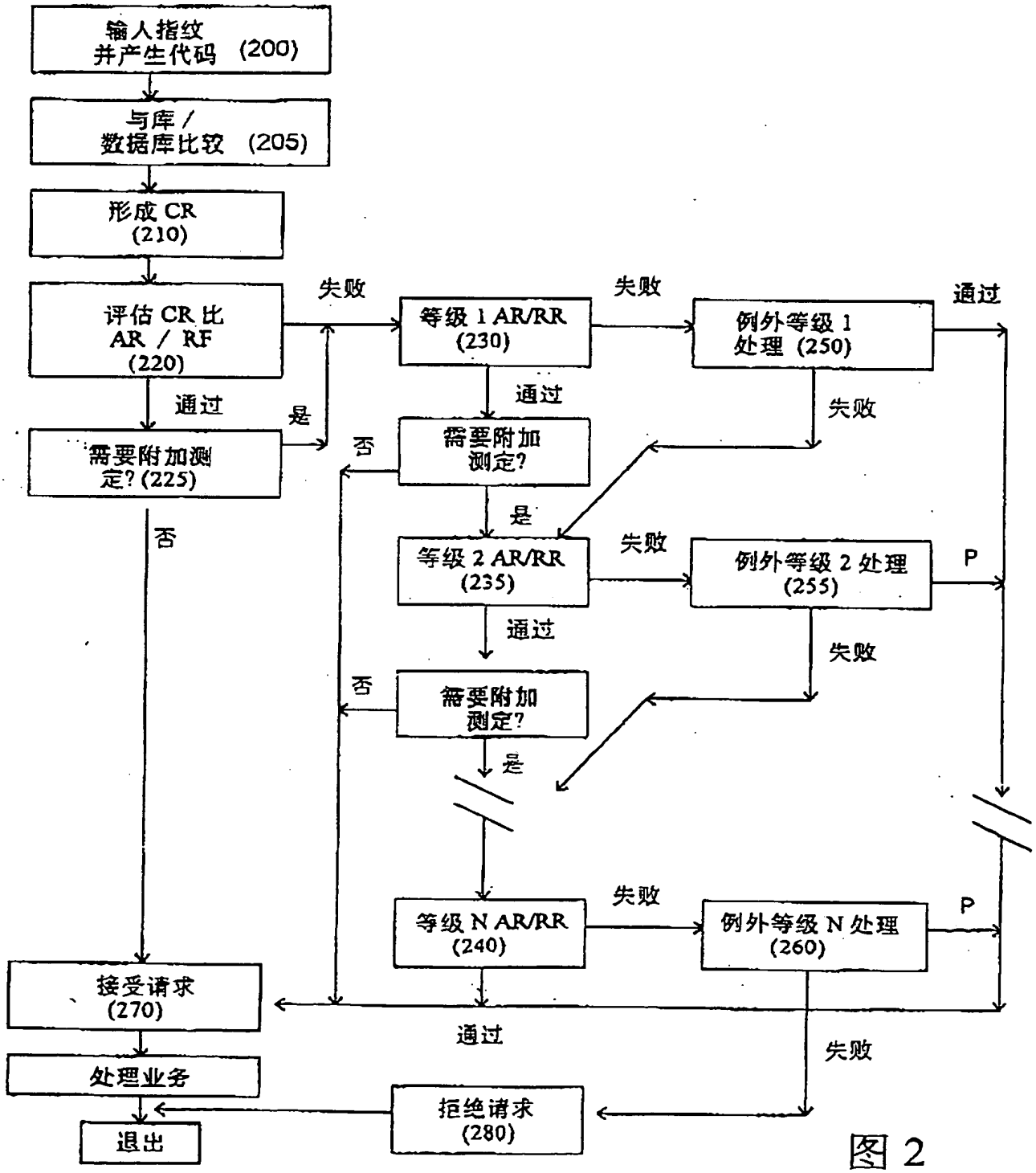
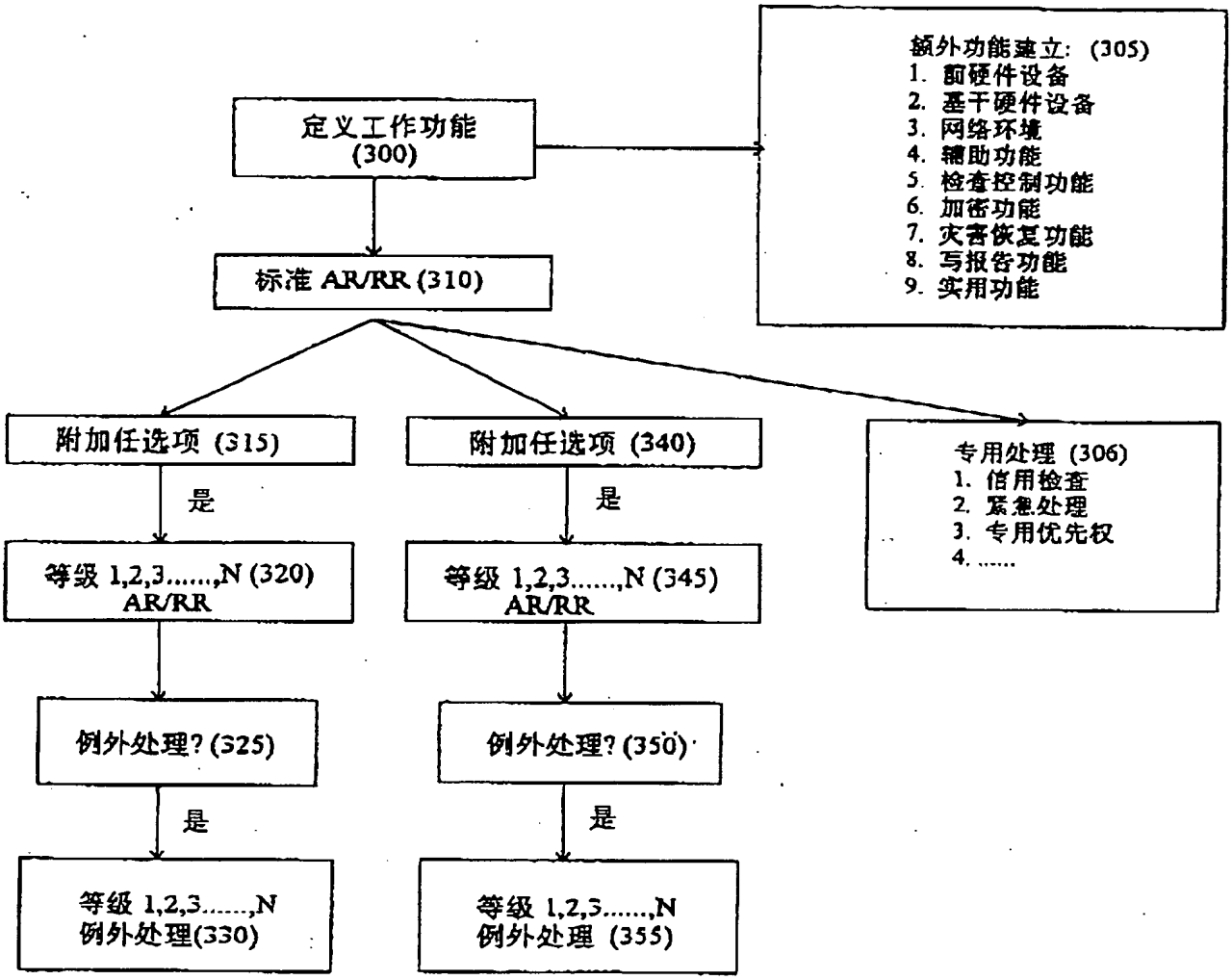

输入指纹
并产生代码 (200)
与库/
数据库比较 (205)
形成 CR
(210)
评估 CR 比
AR / RF
(220)
失败
等级 1 AR/RR
(230)
失败
例外等级 1
处理 (250)
通过
通过
失败
通过
是
需要附加测
定? (225)
否
需要附加
测定?
否
是
等级 2 AR/RR
(235)
失败
例外等级 2 处理
(255)
P
通过
失败
否
需要附加
测定?
是
等级 N AR/RR
(240)
失败
例外等级 N 处理
(260)
P
接受请求
(270)
通过
失败
处理业务
拒绝请求
(280)
退出

图 2

实例: 建立屏幕



用于登记之目的:
根据不同标准用于用户快速建立预有规则和表格

图 3